REMARKS

In an Office Action dated 19 January 2006, the Examiner rejects claims 29-50 (all pending claims). In response to the rejections, Applicant amends claims 29, 33, 35, and 37 as well as respectfully traversing the rejections. Claims 29-50 remain in the Application. In light of amendments and the following arguments, Applicant respectfully requests that the Examiner allow all of the claims and this Application be allowed.

Applicant has amended claim 29 to overcome the §112 rejection. Specifically, Applicant has amended the claim to add the name of the circuitry being modified.

The Examiner rejects claim 1 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Number 5,883,956 issued to Le et al. (Le). In order to maintain a rejection the Examiner has the burden of providing evidence of prima facie obviousness. See MPEP §2143. See also In Re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). In order to prove prima facie obviousness, the Examiner must provide evidence in the prior art of a motivation to combine or modify a reference, a reasonable expectation of success, and **a teaching of each and every claimed element**. Id. *Emphasis added.*

Applicant is stating that the Examiner has **failed to provide** a teaching of a token decryption system in the non-volatile memory that uses the decrypted encrypted initialization data reconfigure the chip once the initialization data is decrypted.

Amended claim 29 recites "token decryption circuitry in said non-volatile memory to decrypt said encrypted initialization data in said encrypted token wherein

said initialization data enables said circuitry in said cryptographic chip to perform encryption and decryption of data for one of said plurality of cryptographic systems." Le does not teach this limitation. Instead, Le merely teaches that initialization and/or configuration data is contained in a non-volatile memory. See Col. 3, lines 15-25. In Le, encrypted configuration data may be received from another source. **Software** then performs decryption and verification of the data. Software sets the enabling bit string after the data is verified. See Col. 11, line 10- Col. 12, line 45. The system in claim 1 actually uses a cryptographic chip to decrypt the data and then re-configures the cryptographic chip with the data. This allows system of claim 1 to be initialized without outside data and without wasting processing time of a processor. Thus, Le does not teach the token decryption system recited in amended claim 29.

The Examiner admits as much in the Office Action. However, the Examiner states that Le would be motivated to modify Le to include encrypted initialization data to make the system more secure. However, the Examiner is reminded that one cannot modify a reference if the reference **teaches away from the modification.** Le does in fact teach away from this premise. Specifically, Le states that storing the initialization data in the non-volatile memory is a disadvantage as stated in the following passage:

> "One approach which allows for customized configuration of an SPU depending upon the application which is being used is through the use of different tables or vectors in Read-Only-Memory (ROM).... **One disadvantage of this method** is that is does not offer the flexibility of allowing a system administrator to dynamically reconfigure an SPU once it is installed in the field. " (Emphasis added) See Col 3, lines 15-25.

Thus, one skilled in the art reading Le would not be motivated to provide encrypted initialization data in a non-volatile memory as Le specifically says this is not desirable. Therefore, the Examiner has provided no valid evidence of a motivation to combine. Thus, Applicants respectfully request that rejection of claim 29 be removed and amended claim 29 be allowed.

Claims 30-32 are dependent from claim 29. Therefore, claims 30-32 are allowable for at least the same reasons as claim 29. Thus, Applicant respectfully requests the rejections of claims 30-32 be removed and claims 30-32 be allowed.

Amended claim 33 recites a method for configuring a cryptographic chip at start-up using the encrypted encryption initialization data that is recited in amended claim 29. Thus, amended claim 33 is allowable for at least the same reasons as amended claim 29.

Claim 34 is dependent from claim 33. Therefore, claim 34 is allowable for at least the same reasons as amended claim 33. Thus, Applicant respectfully requests claim 34 be allowed.

Amended claim 35 recites a program for providing the method for configuring a cryptographic chip at start-up using the encrypted encryption initialization data that is recited in amended claim 29. Thus, amended claim 35 is allowable for at least the same reasons as amended claim 29. Therefore, Applicant requests amended claim 35 be allowed.

Claim 36 is dependent from claim 35. Therefore, claim 36 is allowable for at least the same reasons as amended claim 35. Thus, Applicant respectfully requests claim 36 be allowed.

Amended claim 37 recites a system for providing the method for configuring a cryptographic chip at start-up using the encrypted encryption initialization data that is recited in amended claim 29. Thus, amended claim 37 is allowable for at least the same reasons as amended claim 29. Therefore, Applicant requests amended claim 37 be allowed.

Claim 38 is dependent from claim 37. Therefore, claim 38 is allowable for at least the same reasons as amended claim 37. Thus, Applicants respectfully request claim 38 be allowed.

Claim 39 recites a method for generating an encrypted token including the encryption initialization data recited in amended claim 29. Thus, claim 39 is allowable for at least the same reasons as amended claim 29. Therefore, Applicant requests that claim 39 be allowed.

Claims 40-42 are dependent from claim 39. Therefore, claims 40-42 are allowable for at least the same reasons as claim 39. Thus, Applicant respectfully requests claims 40-42 be allowed.

Claim 43 recites a program for providing the method for generating the encrypted token recited in claim 39. Thus, claim 43 is allowable for at least the same reasons as claim 39. Therefore, Applicant requests that claim 43 be allowed.

Claims 44-46 are dependent from claim 43. Therefore, claims 44-46 are allowable for at least the same reasons as claim 43. Thus, Applicant respectfully requests claims 44-46 be allowed.

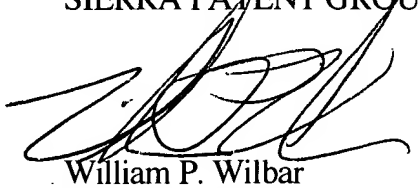
Claim 47 recites a system for providing the method for generating the encrypted token recited in claim 39. Thus, claim 47 is allowable for at least the same reasons as claim 39. Therefore, Applicant requests that claim 47 be allowed.

Claims 48-50 are dependent from claim 47. Therefore, claims 48-50 are allowable for at least the same reasons as claim 47. Thus, Applicant respectfully requests claims 48-50 be allowed.

If the Examiner has any questions regarding this response or the application in general, the Examiner is invited to telephone the undersigned at 775-586-9500.

Respectfully submitted,
SIERRA PATENT GROUP, LTD.

Dated: March 29, 2006



William P. Wilbar
Reg. No.: 43,265

Sierra Patent Group, Ltd.
1657 Hwy. 395, Suite 202
Minden, NV 89423
(775) 586-9500
(775) 586-9550 Fax